



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,665	02/02/2001	Donald B. Johnson	6944-8-1	7060

293 7590 09/12/2005

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave.
Suite 406
Alexandria, VA 22314

EXAMINER

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 09/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/773,665	Applicant(s) JOHNSON ET AL.	
	Examiner Paula W. Klimach	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 12-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 12-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 06/20/05. Applicant added Claims 12-21, and cancelled Claims 1-11. The amendment filed on 06/20/05 have been entered and made of record. Therefore, presently pending claims are 12-21.

Response to Arguments

Applicant's arguments filed 06/20/05 have been fully considered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 12-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography by Schneier in view of the article "New Public-Key Schemes Based on Elliptic Curves over the Ring \mathbb{Z}_n " by Koyama.

In reference to claim 12, Schneier discloses a system wherein the verifier (Bob) obtaining a pair of signature components (d, D), said component being derived from a first (random integer r) and second signature components (B) generated by a signor; the verifier (Bob) calculating a signature component r' (d') from one of said coordinate pairs; and verifying said signature if $r' = r$ ($d = d'$; pages 509-510 Guillou-Quisquater Signature Scheme).

The signature scheme of Guillou-Quisquater does not disclose the use of elliptic curve for calculating the signature.

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair (x_1, y_1) corresponding to said first short term public key using the pair (s, t) and said message M (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

In reference to claim 13 further comprising the step of said verifier receiving (r, s, c) from said signor and converting (s, r, c) to obtain said pair (s, r) (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 14, further comprising the step of said signor converting (s, r, c) to said pair (s, r) and said signor sending said pair (s, r) to said verifier.

Schneier discloses the verifier receiving the three components and converting these into two components (pages 509-510 Guillou-Quisquater Signature Scheme).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to convert the components by the signor. One of ordinary skill in the art would have been motivated to do this because it is a mere calculation that can be performed at either device.

In reference to claim 15 wherein said coordinate pair (x_1, y_1) is calculated using a pair of values u and v , said values u and v derived from said pair (s, r) and said message

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair (x_1, y_1) corresponding to said first short term public key using the pair (s, t) and said message M (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

In reference to claim 16 wherein said coordinate pair (x_1, y_1) is calculated as $(x_1, y_1) = uP + vQ$, wherein P is a point on an elliptic curve E and Q is a public verification key of said signor derived from P as $Q = dP$

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore the recovering of a coordinate pair (x_1, y_1) corresponding to said first short term public key using the pair (s, t) and said message M (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

In reference to claim 17 wherein said value u is computed as $u = s^{-1} \text{ emod } n$ and said value v is computed as $v = s r \text{ mod } n$, e being a representation of said, message m (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 18 wherein e is calculated as $e=H(m)$, $H(\)$ being a hash function of said signor and being known to said verifier (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 19 wherein said coordinate x_1 first converted to an integer x_1 prior to calculating said component r' (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 20 wherein said component r' , is calculated as $r'=x_1 \bmod n$ (pages 509-510 Guillou-Quisquater Signature Scheme).

In reference to claim 21 wherein prior to calculating said component r' , said coordinate pair (x_1, y_1) is first verified, whereby if said coordinate pair (x_1, y_1) is a point at infinity, then said signature is rejected.

Koyama discloses the use of elliptic curve to calculate digital signatures and therefore coordinate pair (x_1, y_1) is a point at infinity, then said signature is rejected (Section 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use elliptic curve as in Koyama in the system of Schneier. One of ordinary skill in the art would have been motivated to do this because the computational speed of the elliptic curve algorithm is faster than that of RSA and therefore for the analogues of RSA.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2135

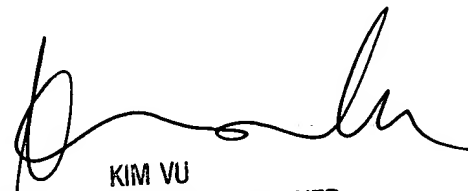
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100